REMARKS

Applicants respectfully request consideration of the subject application as amended herein. This Amendment is submitted in response to the Final Office Action mailed July 8, 2008. Claims 1-32 stand rejected. In this Amendment, claims 1, 20, 31 and 32 have been amended. Claim 7 has been canceled. No new matter has been added.

Examiner Interview

Applicants thank the Examiner for granting an Examiner Interview on September 11, 2008. In the Examiner interview, applicants discussed claim 1 of the present application with reference to U.S. Patent No. 5,835,722 to Bradshaw et al. and U.S. Patent No. 6,233,618 to Shannon. In particular, possible clarifying amendments for claim 1 were discussed, which are reflected in the current claim amendments.

35 U.S.C. §103

The Examiner has rejected claims 1-2, 6-15, 20-21, 24-26 and 31-32 under 35 U.S.C. §103(a) as being unpatentable over Bradshaw (U.S. Patent No. 5,835,722, hereinafter "Bradshaw") in view of Shannon (U.S. Patent No. 6,233,618, hereinafter "Shannon").

Bradshaw describes blocking the use and transmission of vulgar and pornographic material by comparing words typed in a word processor, words in a clipboard, and words typed in an Internet engine to words in various libraries. (Bradshaw, Abstract and col. 6, lines 1-5). Specifically, Bradshaw matches words in a keyboard queue and a clipboard to words in the libraries to initiate blocking routines. (Bradshaw, col. 8, lines 49-55 and col. 10, lines 15-32).

Claim 1, as amended, recites in part "receiving an abstract data structure derived from pre-selected data to be protected, the pre-selected data being stored on a server." In Bradshaw, there is no abstract data structure derived from pre-selected data to be protected. Bradshaw monitors computer operations for creation or transmission of vulgar and pornographic material by comparing the words typed in a word processor and words typed in an Internet search engine to data that is stored in libraries. (Bradshaw, Abstract and col. 6, lines 1-5). The libraries contain lists of prohibited Internet sites, prohibited E-mail addresses, and prohibited words. (Bradshaw, col. 6, lines 5-10). But, Bradshaw's libraries are not abstract data structures derived from pre-selected data to be protected because Bradshaw's libraries are not derived from anything. Bradshaw teaches that the libraries are included as part of a software program installed on a PC and manually modified by a supervisor. (Bradshaw, col. 6, line 64 to col. 7, line 38). In Bradshaw, a company supervisor sets up the libraries by modifying the lists in the libraries during a set-up routine when the program is first installed. (Bradshaw, col. 6, line 64 to col. 7, line 38). Therefore, Bradshaw does not describe deriving an abstract data structure from the pre-selected data to be protected. Thus, Bradshaw does not teach or suggest "receiving an abstract data structure derived from pre-selected data to be protected, the pre-selected data being stored on a server," as stated in claim 1.

Moreover, Bradshaw fails to teach or suggest "searching, locally, text contained in a plurality of documents stored on a plurality of data storage media of the client device for an indication that at least a portion of the pre-selected data stored on the server may be contained in the text of the plurality of documents, *the indication being detected based on the abstract data structure without using the pre-selected data*," as stated in claim 1. (Emphasis added). Bradshaw searches data in a word processor, clipboard application, and Internet search engine *directly for pre-selected data*. Bradshaw's libraries contain lists of prohibited Internet sites, prohibited E-

mail addresses, and prohibited words. (Bradshaw, col. 6, lines 5-10). Specifically, Bradshaw describes that a blocking routine is initiated when words typed in a word processor or in an Internet search engine *match words in the libraries*. (Bradshaw, col. 8, lines 54-55). Since Bradshaw's libraries contain lists of the words being searched for and matched with, in Bradshaw, *pre-selected data is directly used for a search*. In contrast, claim 1 describes that pre-selected data is not used for a search because an abstract data structure is used to detect "an indication that at least a portion of the pre-selected data stored on the server may be contained in the text of the plurality of documents, the indication being detected based on the abstract data structure *without using the pre-selected data*." (Emphasis added). Thus, Bradshaw fails to teach or suggest "searching, locally, text contained in a plurality of documents stored on a plurality of data storage media of the client device for an indication that at least a portion of the pre-selected data stored on the server may be contained in the text of the plurality of documents, the indication being detected based on the abstract data structure without using the pre-selected data," as stated in claim 1.

In addition, Bradshaw fails to teach or suggest "sending, from the client device to the server, a notification of detection of at least a portion of the pre-selected data in the text of at least one of the plurality of documents stored locally on any of the plurality of data storage media of the client device," and cites Shannon for teaching such a limitation. Applicants respectfully disagree.

Shannon does not teach or suggest the limitations missing from Bradshaw. Shannon limits a client's access to information on the Internet. (Shannon, Abstract). In Shannon, clients send requests for web pages, files, and other information to servers. (Shannon, Abstract). A network device, such as a proxy server, analyzes data in the client's request to determine if the request should be forwarded for processing by a server. (Shannon, Abstract). Shannon provides

access control not based only upon content, but rather, based primarily upon the identity of the computers or users making the requests. (Shannon, Abstract).

However, Shannon does not teach or suggest "sending, *from the client device to the server*, a notification of detection of at least a portion of the pre-selected data," as set forth in claim 1. (Emphasis added). Shannon, Figure 1 illustrates *clients* 50 through 53, *servers* 54 through 56, and network link 41 to *network device* 100. (Shannon, col. 5, lines 34-53). Therefore, Shannon distinguishes clients, servers, and network devices as different entities. In Shannon, the client device does not send a notification to a server, but rather a network device sends a notification to the client. (Shannon, col., 14, lines 43-47). Shannon describes that *network device* 100 performs the processing steps to perform access control, including:

> If step 209 does detect an attempt at restricted access to… restricted content, step 214 is executed to send a return notification of denial *to* the user at *the client* computer requesting the restricted data.

(Shannon, col., 13, lines 21-23 and col., 14, lines 43-47, emphasis added). Specifically, Therefore, Shannon describes the network device sending a return notification *to the client device* and fails to teach or suggest not "sending, from the client device to the server, a notification of detection of at least a portion of the pre-selected data," as described in claim 1.

Moreover, nowhere does Shannon teach or suggest "receiving an abstract data structure derived from pre-selected data to be protected, the pre-selected data being stored on a server," as described in claim 1. Shannon also does not teach or suggest "searching, locally, text contained in a plurality of documents stored on a plurality of data storage media of the client device for an indication that at least a portion of the pre-selected data stored on the server may be contained in the text of the plurality of documents, *the indication being detected based on the abstract data structure without using the pre-selected data*," as described in claim 1. (Emphasis added). Hence, Shannon is missing the same limitations as Bradshaw. Accordingly, the cited references,

taken alone or in combination, do not teach or suggest the limitations of the present invention that are included in the following language of claim 1:

> receiving an abstract data structure derived from pre-selected data to be protected, the pre-selected data being stored on a server;
>
> searching, locally, text contained in a plurality of documents stored on a plurality of data storage media of the client device for an indication that at least a portion of the pre-selected data stored on the server may be contained in the text of the plurality of documents, the indication being detected based on the abstract data structure without using the pre-selected data;
>
> detecting locally at least a portion of the pre-selected data in the text of at least one of the plurality of documents stored on any of the plurality of data storage media of the client device; and
>
> sending, from the client device to the server, a notification of detection of at least a portion of the pre-selected data in the text of at least one of the plurality of documents stored on any of the plurality of data storage media of the client device, the client device being a personal computing device.

Similar language is also included in independent claims 20 and 32. Accordingly, the present invention as claimed in independent claims 1, 20 and 32 and their corresponding dependent claims are patentable over the cited references.

Claim 31, as amended, recites in part:

> a plurality of storage media storing an abstract data structure derived from pre-selected data to be protected, the pre-selected data being stored on a server, and a plurality of documents containing text for the client device, the client device being a personal computing device; and
>
> at least one processor coupled to the plurality of storage media, at least one processor executing a set of instructions which cause the processor to search locally the text in the plurality of documents stored on a plurality of data storage media of the client device for an indication that at least a portion of the pre-selected data stored on the server may be contained in the text of the plurality of documents, the indication being detected based on the abstract data structure without using the pre-selected data, and to send, from the client device to the server, a notification of detection of at least a portion of the pre-selected data in the text of at least one of the plurality of documents stored on any of the plurality of data storage media of the client device, the client device being a personal computing device.

As noted above, neither Bradshaw nor Shannon teach or suggest an abstract data structure, an indication being detected based on the abstract data structure without using the pre-selected data, or sending a notification of detection from the client to a server. Therefore, the

cited references, taken alone or in combination, do not teach or suggest the limitations of the present invention that are taught in claim 31. Accordingly, the present invention as claimed in independent claim 31 and its corresponding dependent claims is patentable over the cited references.

Claims 4, 16-19, 22 and 27-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Bradshaw, in view of Shannon, and further in view of Brandt (U.S. Patent No. 5,892,905, hereinafter "Brandt") filed December 23, 1996. Claims 4 and 16-19 are dependent on claim 1. Therefore, claims 4 and 16-19 include the same limitations as claims 1. Claims 22 and 27-30 are dependent on claim 20. Therefore, claims 22 and 27-30 include the same limitations as claims 20. As noted above, Bradshaw and Shannon, taken alone or in combination do not teach or suggest the limitations recited in claims 1 and 20. These features are also missing from Brandt.

Brandt provides a common user interface for a software application accessed via the Internet. A software application runs on a web server computer system. Therefore, similarly to each of Bradshaw and Shannon, Brandt does not teach or suggest the limitations recited in claim 1. Thus, claims 4, 16-19, 22 and 27-30 are patentable for at least the same reasons as given above with respect to claims 1 and 20.

Claims 5 and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Bradshaw, in view of Shannon, further in view of Brandt (US Patent No. 5,892,905, hereinafter "Brandt") filed December 23, 2996, and further in view of Dascalu (US Patent No. 5,958,015) filed October 29, 1996. Claim 5 is dependent on claim 4, which is dependent on claim 1. Therefore, claim 5 includes the same limitations as claim 1. Claim 23 is dependent on claim 20. Therefore, claim 23 includes the same limitations as claim 20. As noted above, Bradshaw and Shannon, taken alone or in combination do not teach or suggest the limitations recited in claims

1 and 20. These features are also missing from Dascalu.

Dascalu teaches a session wall that listens to communications sent over the network. It listens to communication messages exchanged between a client and a server and determines whether the messages can be permitted based on stored access rules. Therefore, similarly to each of Bradshaw and Shannon, Dascalu does not teach or suggest the limitations recited in claims 1 and 20. Thus, claims 5 and 23 are patentable for at least the same reasons as given above with respect to claims 1 and 20.

Applicants respectfully request the withdrawal of the rejections under 35 U.S.C. §103(a) and submit that all pending claims are in condition for allowance, which action is earnestly solicited.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Joan O. Arbolante at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: October 3, 2008

/Joan Obispo Arbolante/
Joan Obispo Arbolante
Reg. No. 58,642

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300